WHAT IS CLAIMED IS:

1. An information processing apparatus comprising:

storage means for storing thereinto an encrypted protective object including a procedure capable of terminating a process operation due to invalidity of a protect code contained in an executable module;

decrypting means for reading said encrypted protective object from said storage means and decrypting said encrypted protective object;

code writing means for causing said protect code to be contained in an executable module generated by linking said decrypted protective object with another object; and

deleting means for deleting said decrypted protective object after said decrypted protective object has been linked with said another object.

2. An information processing apparatus comprising:

storage means for storing thereinto an encrypted protective object including a procedure capable of terminating a process operation due to invalid relationship between a first protect code and a second protect code contained in an executable module;

decrypting means for reading said encrypted protective object from said storage means and decrypting said encrypted protective object;

code generating means for generating said first protect code and said second protect code related to said first protect code;

code writing means for embedding said first protect code into said decrypted protective object, and for embedding said second protect code into said executable module when said executable module is generated by linking with another object said protective object into which said first protect code has been embedded; and

deleting means for deleting said protective object into which said first protect code has been embedded before said second protect code is embedded.

3. An information processing apparatus as claimed in claim 2 wherein:

said code generating means generates both said first protect code and said second protect code from a random number.

4. An information processing apparatus as claimed in claim 2, wherein:

said code writing means adds dummy data to both said first protect code and said second protect code.

5. An information processing apparatus as claimed in claim 3, wherein:

said code writing means adds dummy data to both said first protect code and said second protect code.

6. An information processing apparatus as claimed in claim 1, wherein:

said code writing means encrypts the protect code to be contained in said executable module; and

said protective object includes a procedure for decrypting the encrypted protect code contained in said executable module when said protect code is checked.

7. An information processing apparatus as claimed in claim 2, wherein:

said code writing means encrypts said first protect code and said second protect code both to be contained in said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect codes are checked.

8. An information processing apparatus as claimed in claim 3, wherein:

said code writing means encrypts said first protect code and said second protect code both to be contained in said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect codes are checked.

9. An information processing apparatus as claimed in claim 4,

wherein:

said code writing means encrypts said first protect code and said second protect code both to be contained in said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect codes are checked.

10. An information processing apparatus as claimed in claim 5, wherein:

said code writing means encrypts said first protect code and said second protect code both to be contained in said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect codes are checked.

11. A machine readable storage medium stored with a program used for causing an information processing apparatus to execute a process operation, wherein:

said program causes said information processing apparatus to execute:

a decrypting process operation for decrypting an encrypted protective object to generate a protective object which contains a procedure for terminating a process operation due to invalidity of a protect code included in an executable module;

a linking process operation for linking the protective object produced by said decrypting process operation with another object so as to generate said executable module;

a code writing process operation for containing said protect code into the executable module formed by said coupling process operation; and

a deleting process operation for deleting said protective object generated by said decrypting process operation after said protective object has been linked with said another object.

12. A machine readable storage medium stored with a program used for causing an information processing apparatus to execute a process operation, wherein:

said program causes said information processing apparatus to execute:

a decrypting process operation for decrypting an encrypted protective object to generate a protective object which contains a procedure for terminating a process operation due to an invalid relationship between a first protect code and a second protect code included in an executable module;

a code generating process operation for generating both said first protect code and said second protect code related to said first protect code;

a first code writing process operation for embedding said first protect code into the protective object generated by said decrypting process operation after said decrypting process operation has been executed;

a linking process operation for linking the protective object into which said first protect code is embedded in said first code writing process operation, with another object so as to generate an executable module after said first code writing process operation has been executed;

a second code writing process operation for embedding said second protect code into said executable module generated in said liking process operation after said linking process operation has been executed; and

a deleting process operation for deleting said protective object generated in said decrypting process operation in an interval between said first code writing process and said second code writing process.

13. A storage medium as claimed in claim 12, wherein:

said program causes said information processing apparatus to generate both said first protect code and said second protect code from a random number in said code generating process operation.

14. A storage medium as claimed in claim 12, wherein:

said program causes said information processing apparatus to add dummy data to both said first protect code and said second protect code.

15. A storage medium as claimed in claim 13, wherein:

said program causes said information processing apparatus to add dummy data to both said first protect code and said second protect code.

16. A storage medium as claimed in claim 11, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said protect code to be incorporated into said executable module; and

said protective object includes a procedure for decrypting said encrypted protect code contained in said executable module when said protect code is checked.

17. A storage medium as claimed in claim 12, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first and second protect codes to be incorporated into said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect code are checked.

18. A storage medium as claimed in claim 13, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first and second protect codes to be incorporated into said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect code are checked.

19. A storage medium as claimed in claim 14, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first and second protect codes to be incorporated into said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect code are checked.

20. A storage medium as claimed in claim 15, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first and second protect codes to be incorporated into said executable module; and

said protective object includes a procedure for decrypting said encrypted first protect code and said encrypted second protect code contained in said executable module when said first and second protect code are checked.

21. A machine readable storage medium stored with an object to be process by an information processing apparatus, wherein:

an encrypted protective object is stored into said storage medium; and said encrypted protective object contains a procedure capable of terminating a process operation when there is invalidity in one, or more protect codes contained in an executable module with said protective object incorporated therein.

22. A storage medium as claimed in claim 21, wherein:

in the case that the protect code contained in said executable module is encrypted, said protective object includes a procedure capable of decrypting said encrypted protect code prior to a checking operation of said protect code.

23. A method of generating an executable module, which causes an information processing apparatus to generate said executable module by linking a plurality of objects with each other, comprising the steps of:

generating, by decrypting an encrypted protective object, a protective object containing a procedure for terminating a process operation due to invalidity of a protect code included in an executable module;

generating said executable module by linking said decrypted protective object with other object and writing said protect code; and

deleting said decrypted protective object after linking with said other object.

24. A method of generating an executable module, which causes an information processing apparatus to produce said executable module by

linking a plurality of objects with each other, comprising the steps of:

generating, by decrypting an encrypted protective object, a protective object containing a procedure for terminating a process operation due to an invalid relationship between a first protect code and a second protect code included in said executable module;

generating said first and second protect codes;

embedding said first protect code into said decrypted protective object;

generating said executable module by linking with other object said first-protect-code-embedded protective object;

embedding said second protect code into said executable module; and

deleting said first-protect-code-embedded protective object before embedding of said second protective code.

25. A machine readable storage medium stored with an executable module, said executable module being executed by an apparatus capable of executing an executable module assembled by linking a plurality of objects with each other, wherein:

said plurality of objects each contain a library object, and said library object contains a procedure capable of checking whether or not there is invalidity in at least one protect code and also of terminating a process operation of said executable module in response to said checking result; and

said executable module has at least one protect code embedded thereinto.

26. An entertainment apparatus for executing an executable module generated by linking a plurality of objects with each other, comprising,

in the case that both a first protect code contained in one of said plural objects, and a second protect code are contained in said executable module,

means for checking a relationship therebetween; and

means for terminating a process operation of said executable module when said relationship is invalid.

27. A program product containing a program used to cause an information processing apparatus to execute a process operation, wherein;

said program causes said information processing apparatus to execute:

a decrypting process operation for decrypting an encrypted protective object to generate a protective object which contains a procedure for terminating a process operation due to invalidity of a protect code included in an executable module;

a linking process operation for linking the protective object generated by said decrypting process operation with another object so as to generate said executable module;

a code writing process operation for incorporating said protect code into the executable module generated by said linking process operation; and a deleting process operation for deleting said protective object generated by said decrypting process operation after said protective object has been linked with said another object.

28. A program product containing a program used to cause an information processing apparatus to execute a process operation, wherein:

said program causes said information processing apparatus to execute:

a decrypting process operation for decrypting an encrypted protective object to generate a protective object which contains a procedure for terminating a process operation due to an invalid relationship among a plurality of protect codes included in an executable module;

a code generating process operation for generating both a first protect code and a second protect code related to said first protect code;

a first code writing process operation for embedding said first protect code into the protective object generated by said decrypting process operation after said decrypting process operation has been executed;

a linking process operation for linking with another object the protective object into which said first protect code is embedded in said first code writing process operation so as to generate an execution module after said first code writing process operation has been executed;

a second code writing process operation for embedding said second protect code into said executable module generated in said linking process operation after said linking process operation has been executed; and

a deleting process operation for deleting said protective object generated in said decrypting process operation in an interval between said first code writing process operation and said second code writing process operation.

29. A program product as claimed in claim 28, wherein:

said program causes said information processing apparatus to generate both said first protect code and said second protect code from a random number in said code generating process operation.

30. A program product as claimed in claim 28, wherein:

said program causes said information processing apparatus to add dummy data to both said first protect code and said second protect code.

31. A program product as claimed in claim 29, wherein:

said program causes said information processing apparatus to add dummy data to both said first protect code and said second protect code.

32. A program product as claimed in claim 27, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said protect code used to be contained in said executable module; and

said protective object includes a procedure for decrypting the encrypted protect code contained in said executable module when said protect code is checked.

33. A program product as claimed in claim 28, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first protect code and said second protect code to be incorporated into said executable module; and

said protective object includes a procedure for decrypting the encrypted protect code contained in said executable module when said first and second protect codes are checked.

34. A program product as claimed in claim 29, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first protect code and said second protect code to be incorporated into said executable module; and

said protective object includes a procedure for decrypting the encrypted protect code contained in said executable module when said first and second protect codes are checked.

35. A program product as claimed in claim 30, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first protect code and said second protect code to be incorporated into said executable module; and

said protective object includes a procedure for decrypting the encrypted protect code contained in said executable module when said first and second protect codes are checked.

36. A program product as claimed in claim 31, wherein:

said program causes said information processing apparatus to execute a process operation for encrypting said first protect code and said second protect code to be incorporated into said executable module; and

said protective object includes a procedure for decrypting the encrypted protect code contained in said executable module when said first and second protect codes are checked.

37. A software product containing an object to be generated by an information processing apparatus, comprising:

an encrypted protective object including a procedure capable of terminating a process operation when there is invalidity of a protect code which is contained in an executable module with said software product incorporated thererinto.

38. A software product as claimed in claim 37, wherein:

in the case that the protect code contained in said executable module is encrypted, said software product includes a procedure capable of decrypting said encrypted protect code prior to checking whether or not there is invalidity of said protected code.

39. A software product containing an executable module, which is executed by an apparatus capable of executing an executable module assembled by linking a plurality of objects with each other, wherein:

said executable module has at least one protect code embedded therein; and

said plurality of objects each include a library object which contains a procedure for checking whether or not there is invalidity of the protect code contained in said executable module, and for terminating a process operation of said executable module in response to the checking result.